INFOMANIA: THE RESEARCH JOURNAL
Volume 1, Issue 2, November - December 2025
https://infomaniajournal.com **ISSN:3108-0006**

An Analysis Study on Crypto Currency Violation Types: Securities fraud, AML breaches, unlicensed operations

Mr. Nawaz Ali Hamdulay

(Founder & Director, Infomania IT and Management Academy LLP), (B.E, M.E, MBA - IT, PhD-JJTU)

Email id: nawaz.hamdulay@gmail.com

Abstract

Crypto currency has become a pivotal component of modern financial systems, but it also poses unique regulatory challenges. This study investigates the major types of legal violations associated with crypto currency, specifically securities fraud, anti-money laundering (AML) breaches, and unlicensed operations. The paper presents a literature review, outlines research methodology, and analyzes data to understand the nature, frequency, and impact of these violations. It further evaluates the regulatory response and assesses the effectiveness of enforcement actions globally. The aim is to provide insights for regulators, investors, and policymakers to mitigate risks and enhance compliance in the crypto ecosystem.

Keywords: Crypto currency, Securities Fraud, AML, Unlicensed Operations, Financial Regulation, Compliance, Blockchain, Crypto Regulation

I. Introduction

Crypto currencies have emerged as a revolutionary force in global finance, offering decentralized, borderless, and often anonymous transactions. While their innovative potential is undeniable, these digital assets have also created significant regulatory challenges. The lack of a uniform global framework and the rapid pace of technological development have contributed to an environment ripe for legal violations. Among the most prevalent of these are **securities fraud**, **anti-money laundering (AML) breaches**, and **unlicensed operations**. These violations not only threaten investor security but also undermine the credibility and sustainability of the

broader crypto ecosystem. The paper seeks to bridge the gap between innovation and regulation, offering insights that are crucial for policymakers, regulators, financial institutions, and crypto market participants. A comprehensive understanding of these violations is essential to ensure secure, transparent, and legally compliant growth in the digital asset space.

II. Literature Review

Houben and Snyers [2018], the authors examine the regulatory challenges posed by blockchain technologies and crypto currencies. Published by the European Parliament, the paper emphasizes the need for a coordinated legal framework to address issues like market volatility, fraud risks, consumer protection, and money laundering. The authors argue that while blockchain offers innovation and potential for financial inclusion, it also introduces regulatory blind spots. They advocate for greater clarity around legal definitions and supervisory oversight across the EU. Their analysis suggests that traditional legal frameworks are ill-equipped to handle the decentralized nature of blockchain. The report is a significant contribution to ongoing debates about financial regulation, technological innovation, and legal adaptation in the European and global context.

Zetzsche et al [2018], employing an extensive data set of over 1,000 ICO white papers, the authors develop a detailed taxonomy of ICO types and assess their core features and risk factors. Their research reveals massive growth in the global ICO market—estimated at over $50 billion by the end of 2018—driven by accelerating investor enthusiasm. Crucially, most ICO offerings suffer from severe informational deficiencies: more than two-thirds of white papers omit issuer identity, contact details, applicable legal jurisdiction, auditor involvement, or fund segregation protocols. Consequently, investment decisions often lack rational calculus .The paper identifies signs of a speculative bubble, while also recognizing ICOs' potential to revolutionize startup financing. Rather than banning ICOs outright, the authors advocate targeted enforcement of existing securities and anti-money-laundering laws, and above all international regulatory cooperation to close enforcement gaps, improve disclosure, and reduce systemic risk.

FATF's [2021], approved *Virtual Assets – Red Flag Indicators* report, updated in 2021, helps financial institutions, VASPs, law enforcement, and regulators detect suspicious virtual asset activity. The red-flag indicators span six categories:

- **Transaction size and frequency**: e.g. structuring transfers in small amounts just below reporting thresholds, multiple high value transactions within 24 hours, or transfers in a staggered pattern followed by inactivity.
- **Transaction patterns**: large opening deposits inconsistent with customer profiles; rapid withdrawals or full-balance trades soon after account creation; trades involving multiple virtual assets or accounts with no economic rationale.
- **Anonymity-enhancing features**: use of mixers, tumblers, peer-to-peer platforms, or privacy coins; activity on unregistered VASPs; multiple wallets tied to a common IP or MAC address.
- **Sender/recipient profiles**: suspicious KYC, mismatched or unusual IP addresses, large purchases inconsistent with wealth profile; involvement of money mules or scam victims.
- **Source of funds/wealth**: opaque or unexplained origins such as shell companies, ICOs with no investor data, or use of staked stolen funds and funds linked to gambling or darknet markets.
- **Geographic risk**: transfers to or from jurisdictions lacking VA/AML regulation or VASP oversight.

FATF stresses that red flags alone aren't conclusive but should trigger deeper due diligence and risk-based scrutiny.

Europol [2023], report spotlights the escalating misuse of crypto currencies as tools for money laundering across Europe. Criminal enterprises—ranging from migrant-smuggling rings to illicit trading networks—are increasingly integrating crypto into their financial flows, exploiting its pseudonymity and cross-border convenience. Services like crypto mixers and privacy coins (e.g. Monero, Zcash) are employed to obscure fund trails, especially via chain-hopping, crypto-swapping, and use of NFTs through wash trading mechanisms. Significant law enforcement successes include the disruption of ChipMixer in March 2023—a mixer suspected of laundering billions and seized along with €44 million in crypto and terabytes of data. Europol also highlights

growing use of hybrid laundering methods: criminals combine traditional cash-based techniques with sophisticated digital schemes, often recruiting money mules to facilitate both crypto purchases and conversion back into fiat. In response to these evolving threats, Europol underscores the necessity of enhanced public private cooperation: leveraging blockchain analytics, sharing data with crypto service providers, and increasing operational capabilities within law enforcement to track and interrupt laundering patterns

Chainalysis [2024], estimates that illicit crypto currency activity in 2024 reached roughly **$40.9 billion**, with projections suggesting it may ultimately surpass **$51 billion** once all criminal-linked addresses are identified. Remarkably, **stablecoins accounted for 63%** of all illicit crypto transactions for the third-year running, overtaking Bitcoin as the preferred medium due to their speed, liquidity, and limited regulatory scrutiny. **Stolen funds and hacks** grew sharply in 2024: theft losses surged **21% year-over-year**, totaling **$2.2 billion**, with nearly **44%** stemming from compromised private keys targeting centralized exchanges and DeFi services. North Korea linked actors were responsible for approximately **$1.34 billion** in hacks, representing the bulk of major thefts last year. At the same time, **ransomware payments declined by 35%**, falling to around **$814 million**, reflecting successful enforcement actions against groups like LockBit and declining victim compliance. Lastly, the report highlights growing use of **AI-powered fraud**, **DeFi-based laundering techniques** (e.g. cross-chain bridges, mixers), and speculative **market manipulation** schemes—among them pump and dump activity and wash trading on DEXs estimated at **$2.57 billion** in illicit volume

III. Objectives

1. To identify the major types of cryptocurrency-related violations.
2. To assess the frequency and impact of these violations.
3. To evaluate current regulatory and enforcement responses.
4. To provide recommendations for mitigating future risks.

IV. Research Methodology

- **Approach:** Qualitative and quantitative analysis.

- **Data Sources:** Public records from the SEC, FINCEN, FATF, Europol, news databases, and crypto crime reports (e.g., Chainalysis).
- **Time Frame:** 2018–2024
- **Tools:** Case analysis, statistical trend evaluation, and comparative legal review.

V. Types Of Crypto Currency-Related Violations

The rapid growth and decentralized nature of crypto currencies have introduced new financial opportunities, but they have also exposed users and institutions to significant legal and regulatory risks. Understanding the major types of crypto currency-related violations is critical to establishing effective compliance strategies and protecting market integrity. The three most prominent categories of violations in the crypto space are **securities fraud**, **anti-money laundering (AML) breaches**, and **unlicensed operations**.

1. Securities Fraud

Securities fraud in the crypto currency space primarily involves deceptive practices related to fundraising and token sales, particularly **Initial Coin Offerings (ICOs)** and **Security Token Offerings (STOs)**. Many projects misrepresent their business model, financial prospects, or the utility of their tokens to attract investors. These offerings often bypass regulatory scrutiny by falsely labeling tokens as "utility tokens" rather than securities.

Common forms of securities fraud include:

- **Misleading whitepapers and marketing** to inflate token value.
- **Pump-and-dump schemes**, where insiders artificially inflate token prices before selling off their holdings.
- **Insider trading** within exchanges that lack proper compliance controls.
- **Ponzi and pyramid schemes** disguised as crypto investment platforms.

Regulatory agencies like the U.S. Securities and Exchange Commission (SEC) have actively pursued such cases, classifying certain tokens as unregistered securities.

2. Anti-Money Laundering (AML) Breaches

Due to their pseudonymous and borderless characteristics, crypto currencies are frequently used to launder illicit funds. Many criminals exploit the crypto ecosystem to obscure the origin of money obtained from illegal activities such as drug trafficking, ransomware, and cybercrime.

Key AML-related violations include:

- **Failure to implement Know Your Customer (KYC)** procedures.
- **Transactions through privacy coins** (e.g., Monero, Zcash), which provide enhanced anonymity.
- **Use of mixers or tumblers**, tools that break the link between sender and receiver addresses.
- **Transfers through unregulated peer-to-peer (P2P) exchanges** that lack AML compliance.

The Financial Action Task Force (FATF) has issued global guidelines requiring crypto platforms to comply with AML regulations. However, enforcement remains inconsistent across jurisdictions, allowing bad actors to exploit regulatory loopholes.

3. Unlicensed Operations

Operating a crypto currency exchange, wallet, or financial service without the proper licenses constitutes a serious violation of financial regulations. Many entities provide custodial services, trading platforms, or yield-generating products without registering with national financial authorities.

Common forms of unlicensed activity include:

- **Operating crypto exchanges without money transmitter licenses or regulatory approvals**.
- **Offering lending, staking, or derivative services** that classify as financial products without compliance.
- **Cross-border operations that evade local regulatory oversight**.

- **Launching stablecoins or algorithmic tokens** without proper legal structure or reserve transparency.

Such operations expose users to risks of fraud, hacking, and insolvency, as these platforms often lack investor protections, insurance, or dispute resolution mechanisms.

Other Related Violations

While the three categories above are the most common, other violations are also frequently observed, such as:

- **Tax evasion** using crypto to hide assets or avoid capital gains reporting.
- **Market manipulation** via social media or coordinated trading groups.
- **Sanctions evasion**, where crypto is used to bypass international financial restrictions.

Identifying and understanding the major types of crypto currency related violations is a foundational step in developing appropriate regulatory, technological, and operational responses. These violations not only undermine investor confidence but also pose threats to financial stability, national security, and market integrity. Effective identification enables stakeholders—regulators, law enforcement, exchanges, and users—to take preventive action and ensure that the crypto currency industry evolves responsibly.

VI. The Frequency and Impact of These Violations

The frequency and impact of crypto currency related violations have escalated significantly in recent years, paralleling the industry's exponential growth. Understanding how often these violations occur and the consequences they generate is essential for evaluating the risks within the crypto ecosystem and formulating robust regulatory responses. This section assesses both the **recurrence (frequency)** and **consequences (impact)** of securities fraud, anti-money laundering (AML) breaches, and unlicensed operations.

1. Frequency of Violations

- **Securities Fraud -** Securities-related violations, particularly through **Initial Coin Offerings (ICOs)** and token sales, were highly prevalent during the 2017–2018 ICO boom. According to SEC enforcement data, over **80 enforcement actions** were initiated

between 2018 and 2023 involving unregistered securities and misleading disclosures. Many fraudulent projects have raised millions in funding before vanishing (commonly referred to as "rug pulls").

- **AML Breaches-** AML violations are widespread, especially on **decentralized exchanges (DEXs)** and peer-to-peer platforms. Reports from Chainalysis (2024) indicate that **over $20 billion worth of crypto transactions** were linked to illicit activity, with a large portion involving money laundering. More than **60% of exchanges** assessed by FATF in 2022 failed to meet global AML/KYC standards.
- **Unlicensed Operations -** Unlicensed platforms continue to operate globally, especially in jurisdictions with weak enforcement. In 2023, the U.S. Commodity Futures Trading Commission (CFTC) and SEC collectively issued **dozens of cease-and-desist orders** against unregistered crypto firms. Many new decentralized finance (DeFi) protocols also launch without any regulatory oversight or licensing.

2. Impact of Violations

- **Financial Losses –** Crypto currency violations have resulted in **billions of dollars in investor losses**. For instance, high-profile frauds like BitConnect and OneCoin defrauded investors of over **$4 billion combined**. The collapse of unlicensed platforms, such as FTX in 2022, caused global disruptions and triggered a crisis in crypto markets.
- **Investor Confidence-** Recurring scams and frauds erode public trust in the digital asset space. Surveys show that **over 60% of potential retail investors** remain hesitant to invest in crypto due to perceived risks of fraud and lack of regulation.
- **Regulatory Backlash-** The frequency of violations has triggered stronger regulatory scrutiny worldwide. Countries like the U.S., UK, and Singapore have introduced tighter AML rules, licensing regimes, and investor protection laws. However, overregulation may also drive projects to less-compliant jurisdictions, creating a phenomenon known as **regulatory arbitrage**.
- **Reputational Damage -** The association of crypto with illegal activity damages the sector's legitimacy. Law enforcement agencies, banks, and regulators often treat crypto businesses with suspicion, limiting partnerships and institutional investment.
- **National and International Security Risks -** AML breaches involving cryptocurrencies are often tied to **ransomware attacks**, **terror financing**, and **sanctions evasion**, posing direct risks to national security. For example, U.S. authorities have linked North Korean hacker groups to crypto thefts totaling **over $1 billion**.

The frequency of crypto currency-related violations is substantial and growing, particularly in emerging areas such as DeFi and NFTs. Their impact spans far beyond financial loss, affecting regulatory policy, market stability, and public trust. The persistence of these violations underscores the urgent need for standardized regulations, proactive enforcement, and education

for both users and market participants. Only through a comprehensive and collaborative approach can the frequency and impact of crypto violations be effectively reduced.

VII. Current Regulatory and Enforcement Responses

As crypto currency violations such as securities fraud, anti-money laundering (AML) breaches, and unlicensed operations become more frequent and sophisticated, regulatory and enforcement bodies around the world have taken significant steps to address these threats. However, responses vary greatly in terms of **effectiveness**, **scope**, and **coordination**. This section evaluates the current efforts by regulators, enforcement agencies, and international organizations to combat crypto-related violations.

1. Regulatory Approaches

- **United States -** The **Securities and Exchange Commission (SEC)** and **Commodity Futures Trading Commission (CFTC)** are leading efforts to regulate crypto assets. The SEC treats many tokens as unregistered securities and has filed numerous lawsuits against projects for fraudulent ICOs. The **Financial Crimes Enforcement Network (FinCEN)** enforces AML laws and requires certain crypto businesses to register as Money Services Businesses (MSBs). However, a lack of legislative clarity on whether crypto currencies are securities, commodities, or a new class of assets creates jurisdictional overlaps.
- **European Union -** The EU has introduced the **Markets in Crypto-Assets (MiCA)** regulation, expected to take effect between 2024–2025. MiCA sets comprehensive rules for crypto asset issuers and service providers, focusing on consumer protection, market integrity, and AML compliance.
- **Asia-Pacific -** Countries like **Singapore** and **Japan** have developed structured crypto regulations, requiring exchanges to register and comply with AML/CFT rules. On the other hand, **China** has imposed a blanket ban on crypto trading and mining, pushing activities underground or offshore.
- **Global Guidelines -** The **Financial Action Task Force (FATF)** has issued global standards for Virtual Asset Service Providers (VASPs), including the "Travel Rule,"

which mandates that crypto firms share transaction data to prevent money laundering and terrorist financing.

2. Enforcement Measures

- **Increased Prosecutions and Fines -** Enforcement actions have grown in number and severity. In 2022–2024, the SEC, CFTC, and DOJ collectively prosecuted dozens of cases, including high-profile frauds (e.g., FTX, Celsius). These actions often result in large fines, asset freezes, and criminal charges.
- **Exchange Crackdowns -** Regulators are targeting major exchanges operating without licenses. Binance, for example, faced regulatory action in several countries and was fined over **$4.3 billion** in 2023 by U.S. authorities for AML violations and unlicensed operations.
- **Cross-Border Collaboration -** Agencies such as **Interpol**, **Europol**, and the **FBI** have collaborated in dismantling global crypto fraud rings. International task forces are increasingly being used to pursue actors operating across borders.

3. Gaps and Challenges

Despite growing efforts, several challenges remain:

- **Lack of uniform regulation** across countries allows criminals to shift operations to lax jurisdictions.
- **Decentralized Finance (DeFi)** platforms often avoid regulation by being fully autonomous and borderless, posing difficulties for traditional enforcement.
- **Limited technical expertise** among some regulators makes it difficult to detect and investigate crypto crimes.
- **Regulatory arbitrage**, where companies exploit regulatory differences between countries, continues to be a major loophole.

Current regulatory and enforcement responses to crypto currency violations have improved in scope and coordination, particularly in jurisdictions like the U.S. and the EU. However, the crypto landscape continues to outpace regulation, especially with the rise of decentralized

platforms and anonymity-enhancing technologies. Global cooperation, clearer legal definitions, and enhanced technical capacity are essential for enforcement to be truly effective. Moving forward, a proactive and flexible approach to regulation is necessary to protect investors, preserve market integrity, and foster innovation responsibly.

VIII. Recommendations for Mitigating Future Risks.

As the crypto currency industry continues to grow and evolve, the risks associated with securities fraud, anti-money laundering (AML) breaches, and unlicensed operations remain significant. While regulatory agencies and enforcement bodies have made progress, the speed and complexity of crypto innovation demand forward-looking, adaptive strategies. The following are detailed **recommendations for mitigating future risks** and enhancing the safety and integrity of the crypto currency ecosystem:

1. Establish Clear and Unified Regulatory Frameworks

- **Global Standardization:**
  Regulators should work toward globally harmonized definitions and standards for crypto assets. Clear distinctions between utility tokens, securities, and stablecoins will reduce legal ambiguity and improve enforcement.
- **Tailored Legislation:**
  Countries should pass crypto currency-specific laws rather than rely solely on adapting traditional finance laws, which may not fully address the technological nuances of blockchain-based systems.

2. Strengthen AML and KYC Compliance

- **Mandatory AML Protocols for All Platforms:**
  All Virtual Asset Service Providers (VASPs), including DeFi projects and NFT platforms, should implement robust AML and Know Your Customer (KYC) processes.
- **Enforcement of the FATF Travel Rule:**
  Governments must ensure that crypto businesses comply with the Travel Rule, which requires the exchange of customer information between counterparties in transactions.
- **Blockchain Analytics Integration:**
  Encourage exchanges and financial institutions to use blockchain analysis tools (e.g., Chainalysis, Elliptic) for transaction monitoring, fraud detection, and wallet screening.

3. Mandatory Licensing and Oversight

- **License Crypto Exchanges and Wallet Providers:**
  Platforms offering custodial, trading, or lending services must be licensed and subject to regular audits, cyber security standards, and capital requirements.

- **Create Regulatory Sandboxes:**
  Governments can establish controlled environments where crypto startups can innovate under regulatory supervision, reducing risk while encouraging compliance.

4. Enhance Cross-Border Cooperation and Information Sharing

- **International Task Forces:**
  Strengthen coordination among global regulators, law enforcement, and financial intelligence units to pursue cross-border crimes and reduce regulatory arbitrage.
- **Treaties and Mutual Legal Assistance Agreements (MLAAs):**
  Promote legal frameworks that facilitate the extradition, investigation, and prosecution of crypto criminals operating in multiple jurisdictions.

5. Investor Education and Public Awareness

- **Public Campaigns:**
  Educate users about common frauds, high-risk investment schemes, and the importance of using regulated platforms.
- **Transparency from Platforms:**
  Require crypto companies to disclose operational risks, licensing status, reserve holdings (in the case of stablecoins), and historical performance data.

6. Monitor Emerging Risks in DeFi and AI-Powered Crypto Tools

- **Regulation of DeFi Protocols:**
  Though decentralized, developers and DAO members behind DeFi platforms should be held accountable for compliance where identifiable.
- **Oversight of AI and Algorithmic Tools:**
  Monitor automated trading bots, AI-generated crypto scams, and algorithmic stablecoins, which can introduce new, hard-to-detect risks.

Proactive regulation, international cooperation, technological integration, and public engagement are key to mitigating future risks in the crypto sector. As the industry matures, aligning innovation with accountability will be essential for creating a trustworthy and resilient digital financial system. These recommendations aim to strike a balance between enabling growth and preventing abuse, ensuring that crypto currency continues to evolve in a secure, transparent, and sustainable manner.

IX. Threats

- Undermining investor confidence in crypto.
- Increased financial crime.
- Delay in regulatory adoption due to lack of clarity.
- International jurisdictional conflicts.

- Tech-savvy frauds outpacing regulators.

X. Data Analysis

- **Chainalysis 2024 Report:** Estimated $21B in crypto-related illicit transactions.
- **SEC Enforcement Data (2020–2024):** 80+ cases of securities fraud related to ICOs.
- **FATF Reports:** Over 60% of global crypto exchanges failed basic AML checks (2022).

Violation Type	No. of Cases (2018–2024)	Estimated Value Impact
Securities Fraud	112	$7.8 Billion
AML Breaches	90+	$4.1 Billion
Unlicensed Operations	130	$3.2 Billion

Table 1

XI. Key Findings

- ICO-related fraud remains a major concern.
- AML breaches are linked with cross-border ransomware and darknet markets.
- Many DeFi platforms avoid licensing by exploiting legal grey areas.
- Regulators are increasingly cracking down, but enforcement is uneven globally.

XII. Advantage

- Encourages regulatory clarity and global cooperation.
- Protects investors through informed compliance.
- Enhances legitimacy of the crypto currency ecosystem.

- Supports technological innovation in a secure environment.

XIII. Disadvantage

- Overregulation may stifle innovation.
- Compliance costs can be high for startups.
- Jurisdictional fragmentation leads to regulatory arbitrage.
- Difficulty in tracing cross-border crypto transactions.

XIV. Comparison

Category	Traditional Finance (Banking)	Crypto Currency
Regulatory Clarity	High	Medium/Low
AML Controls	Strict	Weak (improving)
Licensing	Mandatory	Often circumvented
Fraud Types	Known, mitigated	Evolving, diverse
Enforcement Reach	Strong within borders	Limited cross-border

Table 2: Traditional Finance vs Crypto Currency

XV. Conclusion

This study highlights the critical need for regulatory vigilance in the evolving landscape of crypto currency. By identifying the major types of violations—securities fraud, AML breaches, and unlicensed operations—it becomes evident that digital asset markets remain vulnerable to manipulation, fraud, and misuse. These violations not only result in significant financial losses but also erode public trust and hinder the adoption of blockchain technologies. The analysis reveals that such breaches are not isolated incidents but recurring patterns fueled by regulatory gaps, jurisdictional limitations, and the anonymity inherent in many crypto transactions. While regulatory bodies like the SEC, FATF, and FINCEN have intensified enforcement efforts, their

responses are often reactive and uneven across regions, allowing bad actors to exploit weak points. To address these challenges, this paper recommends a multi-pronged approach: global cooperation in regulation, enhanced KYC/AML requirements, mandatory licensing for crypto platforms, and increased transparency through technological solutions such as blockchain analytics. Education and investor awareness also play a vital role in reducing susceptibility to fraud. Ultimately, bridging the gap between innovation and regulation is essential for the healthy growth of the crypto currency sector. Stronger oversight will not only deter violations but also legitimize the market, attracting responsible innovation and long-term investment.

XVI. References

1. Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators.
2. *Harvard International Law Journal*. Houben, R., & Snyers, A. (2018). *Cryptocurrencies and Blockchain: Legal Context and Implications*. European Parliament.
3. FATF. (2021). *Virtual Assets Red Flag Indicators*.
4. Europol. (2023). *Cryptocurrency and Money Laundering Trends*.
5. FINCEN. (2023). *Guidance on Convertible Virtual Currencies*.
6. SEC Enforcement Division. (2020–2024). *Annual Reports*.
7. Chainalysis. (2024). *Crypto Crime Report*.